



# National Webcast Initiative

**June 22, 2004**

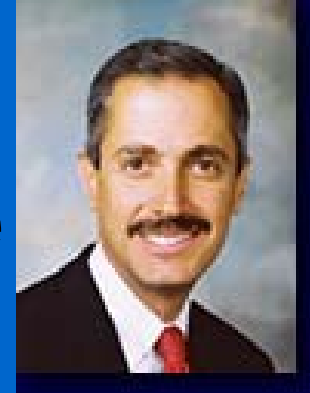
**3:00pm – 4:00pm Eastern**

**National Webcast Initiative**





# National Webcast Initiative



*William F. Pelgrin*

- *Joint Partnership between MS-ISAC and DHS US-CERT*
- *Coordinated through the New York State Office of Cyber Security and Critical Infrastructure Coordination and*
- *the New York State Forum*

**National Webcast Initiative**





# Current Listing of Vendors Interested In Participation

- Accenture
  - AT&T
  - Aon
  - Computer Associates
  - CDW-G
  - CGI
  - CMA
  - D&D Consulting
  - Ernst & Young
  - Gartner
  - HP
  - IIC
  - Jay Dee Systems
  - Keane
  - Microsoft
  - Nortel Networks
  - Novell
  - NYSTEC
  - Oracle
  - SAIC
  - SAS
  - Sybase
  - Symantec
  - Veritas
- This listing will continue to evolve over time*

**National Webcast Initiative**





# Webcast Attendees

- Federal Government
- 44 states
- 120 local governments
- Academia
- International- Canada

**National Webcast Initiative**





# Today's Agenda

**3:00pm-3:15pm**

- **Introduction of Cyber Security Webcast Program**
  - **William Pelgrin**, Chair of the Multi-State ISAC; Director, New York State Office of Cyber Security and Critical Infrastructure Coordination
- **Opening Remarks**
  - **Howard Schmidt**, Chair, National Cyber Security Summit Awareness Task Force; Vice President and Chief Information Security Officer, eBay
  - **Amit Yoran**, Director, National Cyber Security Division, US Department of Homeland Security

**3:15pm-4:00pm**

- **Cyber-Security: Three Things You Should Have Done Yesterday and Three Things You Should Do Today**
  - **Barbara Chung**, Senior Technology Specialist, National Technology Team, Microsoft Corporation

**National Webcast Initiative**





# National Cyber Security Webcast Initiative



National Strategy to Secure Cyberspace - February 2003 Howard Schmidt

*To engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact.*

- Town Hall Sessions Across the Country
  
- National Cyber Security Summit Awareness Task Force – December 2003

charged with implementing the *National Strategy*

- Five Task Forces established:
  - Awareness and Education
  - Cyber Security Early Warning
  - Corporate Governance
  - Technical Standards/Common Criteria
  - Software

**National Webcast Initiative**





# National Cyber Security Webcast Initiative



*Howard Schmidt*

- National Cyber Security Summit Awareness Task Force
- The Webcast Initiative is a joint partnership between US-CERT and the Multi-State ISAC
- Webcast sessions will feature variety of cyber security topics – technical and non-technical
- Goal is to conduct four to six sessions annually
- Sessions will be archived
- Collaborative effort with the vending community

**National Webcast Initiative**





# US-CERT



*Amit Yoran*

US-CERT is, as a public-private partnership, **charged with improving computer security and preparedness and response to cyber attacks**. US-CERT provides a mechanism to link public and private cooperative efforts to help protect and maintain the continuity of our Nation's infrastructures.

The US-CERT Watch is the nation's **focal point for preventing, protecting against, and responding to cyber security threats and vulnerabilities**. The Watch interacts with all federal agencies, private industry, the research community, state and local governments, and others on a 24x7 basis to disseminate reasoned and actionable cyber security information.

**National Webcast Initiative**







# US-CERT



*Amit Yoran*

**US-CERT and the Multi-State ISAC are working together on a number of programs**, including this webcast series, to help enhance our Nation's cyber security readiness and response. The Multi-State ISAC has recently become a member of the US-CERT portal, which provides a secure mechanism for sharing information between and among partners, improving cyber preparedness, readiness and response capabilities.

**US-CERT also hosts a public website, at [www.us-cert.gov](http://www.us-cert.gov), which provides a wealth of information regarding cyber security** – helpful tips for protecting against cyber security threats; cyber security alerts and bulletins, as well as the ability to sign up to receive free cyber security alerts via email.

**National Webcast Initiative**





## Three Things You Should Have Done Yesterday and Three Things You Should Do Today



**Barbara Chung, CISSP, CISM**  
**Sr. Security Specialist**  
**National Technology Team**  
**Microsoft Corporation**

**National Webcast Initiative**





# Agenda

- Threatscape and General Trends
- 3 Thing You Should Have Done
- 3 Things You Should Do

**National Webcast Initiative**





## CHALLENGES

# Threatscape

- **Visible threats:** Viruses and Worms
- **Private threats:** Rootkits, Trojans, Backdoors, Spyware...

...Both classes of threats are complementary: either one may be used to effect the other

Common theme of both is compromise of maximum number of machines

**National Webcast Initiative**

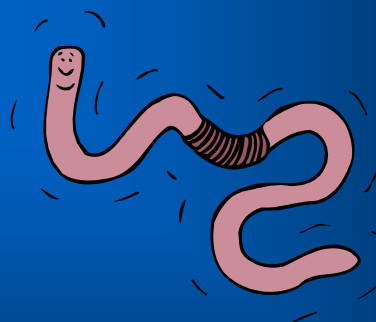




## CHALLENGES

# Visible Attacks: Viruses and Worms

- Usually follow publication of exploit
- May follow release of patch
- Payload can be a private threat
- Initial infection via unpatched machines, unfiltered email, or social engineering



**National Webcast Initiative**





## Tip: Cleaning Viruses and Worms

Once an attacker has obtained administrative rights, you can no longer trust the machine, or the data on it—resist the temptation to try to clean it: **reformat the system drive, rebuild and restore data from backup.**

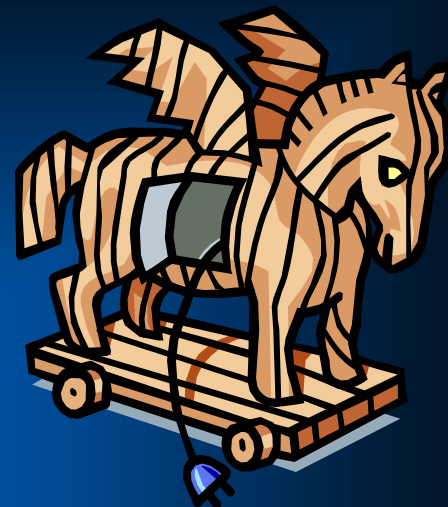
**National Webcast Initiative**





## CHALLENGES

# Private Attacks



- Rootkits, Trojans, Backdoors, etc.
  - Difficult to detect, may go undetected for long periods
  - Popular in 'stealth hosting' schemes
  - Initial method of infection: unpatched machines, poorly configured machines, weak passwords, rogue admins

**National Webcast Initiative**







Computing Networks (TechNews.com) -

Help Search Favorites  
onpost.com/wp-dyn/articles/A8995-2004Apr13.html  
PageRank AutoFill  
computers Search Web

PRINT EDITION | Subscribe to The Washington Post  
Discussions | Photos & Video  
JOBS | CARS | REAL ESTATE  
Top 20 E-mailed Articles

ost.com

TS | ARTS & LIVING | ENTERTAINMENT  
Web by Google

washingtonpost.com

the right candidate. Right now.

Sign Up: [Free Daily Tech E-letter](#)

## Hackers Strike Advanced Computing Networks

By Brian Krebs  
washingtonpost.com Staff Writer  
Tuesday, April 13, 2004; 5:40 PM

Hackers infiltrated powerful supercomputers at colleges, universities and research institutions in recent weeks, disrupting one of the nation's largest online research networks for several days and raising concerns among security experts that the compromised Web sites or networks used to attack specific Web sites or

advertisement

### Cyber-Security

- [Microsoft Finds New Windows Security Flaws](#) (The Washington Post, Apr 14, 2004)
- [A Need for Greater Cybersecurity](#) (The Washington Post, Apr 12, 2004)
- [Worm Triggers Attacks on File-Trading Services](#) (The Washington Post, Apr 10, 2004)
- [More Security News](#)

News.com  
gy Home  
ch  
olicy  
opyright  
ybercrime  
-Taxes  
FCC  
-ICANN  
Security  
ent IT







# Tip: Detecting Rootkits

Rootkits are designed to be invisible, to report incorrect state information to the administrator

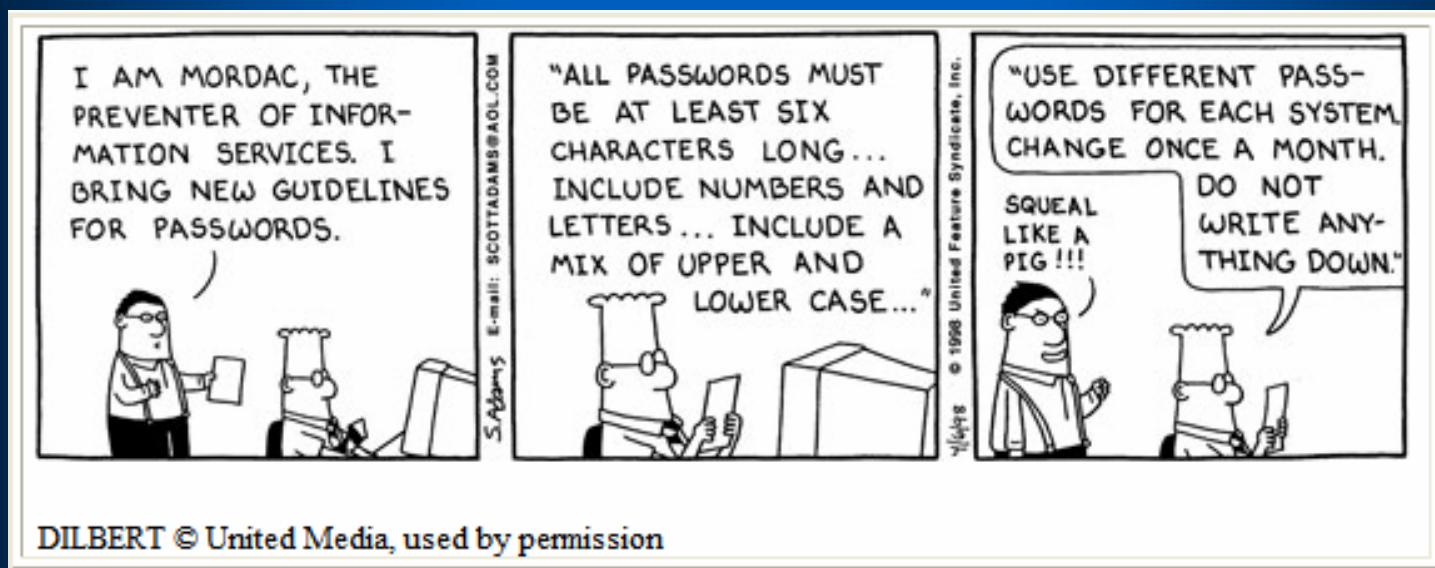
- Be suspicious if you see:
  - Degraded performance or random reboots, anything unusual
- Detection is difficult - get forensic help if you think you're compromised
- **Prevention is the only real solution: manage your environment!**





## CHALLENGES

# Passwords according to Mordac, Preventer of Information Services





## CHALLENGES

# Passwords

- Crackers are ubiquitous & technology is more dangerous
- Compromise of supercomputers and large P2P networks could put serious power in hands of an attacker

**National Webcast Initiative**





# Tip: Use Passphrases

My son John: He would eat 5 bags of  
Oreos @ school if Ms. Jones let him

=

MsJ:Hwe5boO@siMJlh

it's much more difficult to crack and easier  
to remember than:

10F@p:s1

\*this won't work for old Windows clients (authentication will  
break!)

**National Webcast Initiative**





## CHALLENGES

# General Trends

- More of same, only:
  - Vulnerabilities discovered more quickly
  - Faster exploits
  - More complex, more difficult to detect
- Most common method of entering the network:
  - Unpatched machines
  - Weak passwords
  - Social engineering
- Expect it to get worse

**National Webcast Initiative**





## CHALLENGES

# Good Assumptions

- The attacker may know the vulnerability before you do
- The attack may be too fast to detect/stop
- The attack may be silent
- The attacker may have the capability to marshal substantial resources to use against you.





## CHALLENGES

# Defense in Depth

- Force the attacker to compromise several layers of defense in order to be successful
- But where to start?





# 3 things you should have done yesterday...

- ✓ Define a Security Strategy
- ✓ Employ Efficient Patching
- ✓ Implement Effective Password Management

**National Webcast Initiative**







3 THINGS YOU SHOULD HAVE DONE YESTERDAY

## Define 'Security'

- Classic Definition is 'CIA'
  - Confidentiality
  - Integrity
  - Availability
- Each organization must have a clear vision of what they ultimately wish to accomplish

National Webcast Initiative





3 THINGS YOU SHOULD HAVE DONE YESTERDAY

# Five Trustworthy Assurances

- My identity is not compromised
- Resources are secure and available
- Data and communications are private
- Roles and accountability are clearly defined
- There is a timely response to risks and threats

**National Webcast Initiative**



**3 THINGS YOU SHOULD HAVE DONE YESTERDAY**

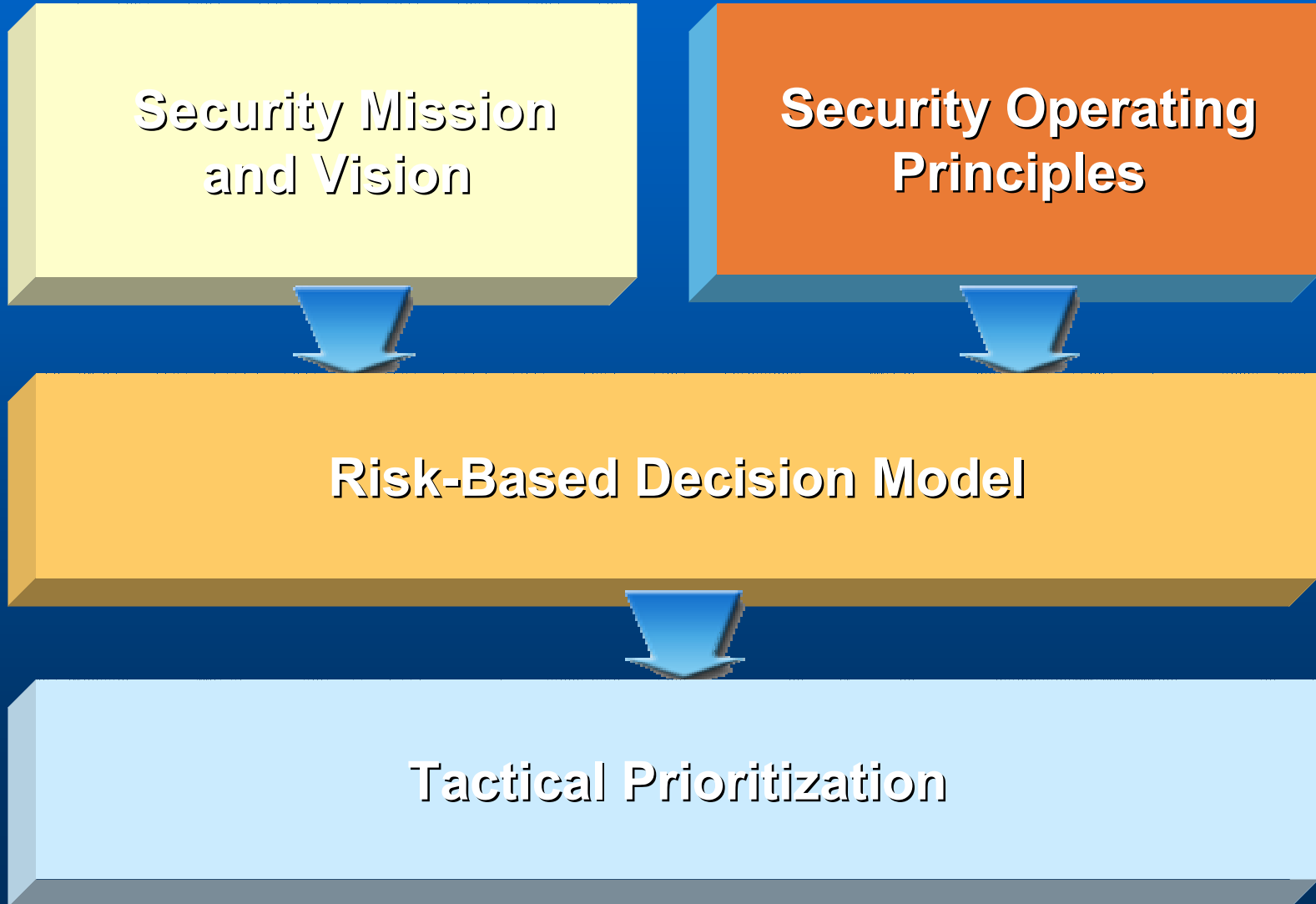
# Security Strategy

Security Mission  
and Vision

Security Operating  
Principles

Risk-Based Decision Model

Tactical Prioritization





3 THINGS YOU SHOULD HAVE DONE YESTERDAY

# Patching

Unpatched machines represent the most common vector for both visible and private attacks

- *Efficient* patching processes

- Which machines are/are not patched
- How long it takes to deliver patches
- Who is responsible

- Crises

- How do you call a crisis, and who calls it? Know everyone's role in the response.
- Practice

National Webcast Initiative





3 THINGS YOU SHOULD HAVE DONE YESTERDAY

# Password Management

- First of all understand that the problem is critical
- Strengthen existing password policy
- Explore strong authentication
  - 2-factor for VPN users and admins in place
- Remember that you will be attacked at the point of your weakest link: security policy must be consistent across the organization

National Webcast Initiative





## 3 things you should do today...

- ✓ Implement Baseline Security
- ✓ Secure the edge against intruders
- ✓ Secure the internal network against malicious authenticated users

**National Webcast Initiative**





3 THINGS YOU SHOULD DO TODAY

# Baseline Security

- Assess your environment
  - Security is based on risk assessment--you can't assess risk if you don't know what it is or what it does
- Integrate threat modeling into your business processes
- Create and distribute standard builds
- Create standard configurations for various classes of machines
- Automate enforcement and auditing
- Establish documentation as ongoing part of engineering and operations

**National Webcast Initiative**





3 THINGS YOU SHOULD DO TODAY

# Secure the Edge

- First of all know where the edges are
- Authenticate all remote and local connections (wired and wireless)
- Where possible, assess security state of the machine before it is allowed on the network (network quarantine)
- See References for tools and technologies

**National Webcast Initiative**







3 THINGS YOU SHOULD DO TODAY

# Secure Internal Network

- Malicious or careless authenticated users represent a large portion of successful compromises; remember that firewalls have not proven to be terribly useful against worms
- Treat unmanaged machines as belonging to the Internet at large
  - Protect at the network level with IPSec protocol
  - Require 2-factor authentication for administrators

**National Webcast Initiative**





# Summary

## Reactive security is a bad bet

- Protect and audit all privileged accounts
- Use the strongest authentication that you can
- Develop a defense-in-depth security strategy
- Lastly, remember that physical access to a server trumps all security!





- **Thank you for participating**
- Future webcast sessions will offer a variety of topics
- Please remain online to participate in an interactive series of survey questions
- Written Q and A to the presenters is available for the next 15 minutes

**National Webcast Initiative**

